1. Classic DoS TCP flooding attack
Flooding can be between 2 peers. Handshake needs to be done.

- Attacker sends syn ack msg
  - For every syn messages sent in flood the server sets up buffer, filling memory
  - All syn messages come from spoofed source addresses, for example, a false IP, or computer not interested in TCP communications
  - Clients do not expect a syn ack messages, because they didn’t initiate, so they will not be responding
  - So server thinks this is breach in communication, problem with a connection
  - Memory is getting reserved for those syn ack messages for clients that never existed
  - Legitimate clients can not be served

- Eventually the server will time out, gives up on TCP connection and releases the buffer
  - TCP Protocol is very robust
  - Over and over

- Attacker can attack number of clients
  - Distributed DoS attack

- Several defences have been created
  - 1. Prevent spoofed IP from reaching you
  - 2. Using cookies to prevent buffer overload

- ICMP flood
  - Sends ICMP packets

Socrative:
- Is there a flood attack that uses the UDP as apposed to TCP (SYN flood)? If so is it more or less of a threat/harder to detect that TCP flood?

UDP is a different streaming type of communication, doesn’t care if it’s delivered reliably or correctly. It will not be persistent as TCP, not saved, etc. UDP is ideal as real time. So it is less widely used, not many applications that uses UDP, not many attacks out there.

- is there where botnets and IOT devices, due to their weak security, often come into play? (SYN spoofing, DOS)

Botnets can use not only laptops, but IOT devices can form a botnet. Often come into play, not necessarily because of their weak security. They can be fairly powerful devices too. For example, in industrial settings, monitoring devices, etc.
2. DDoS attacks and Zombies/Botnets

- Have limited success if from single source
  - Limited upload speed etc.
  - Usually need multiple systems, PC Stations, IOT Devices, attacking congruently on a single victim
- Most DoS attacks are Distributed Denial Of Service Attacks
- Attack the single victim
  - Identify the machines with vulnerability, so they can be compromised and install malicious software and turn them into Zombies
  - Zombie machines are under the control of the Attacker machine, allowing the attack to branch and expand, form layers
  - Attacker makes Zombie Handler machines that connected to Multiple zombies, known as Agent Zombies.
    - So Handler Zombies can trigger Agent Zombies that will set up attack traffic towards a Target
    - This branching known as a botnet, consisting of bots, with help of automated tools
- Botnet mostly used for DoS, but can also be used for cracking passwords
- Very difficult to do something about
  - We can identify Agents, but we don’t know who that attacker is,
  - Target sees multiple attacking bots, but can’t take owner of a bot to court, that are controlled remotely
  - Bots can be in another country, can go very deep, span across wide, etc.
  - Those bots are probably zombies and primary user had no affiliation
  - Attacker doesn't actually connect to target. So cannot be traced, prosecuted, may not already exist within botnet
  - Mirai network - we don’t know extent of the botnet. But it can also be a subset of the network

Socrative:

- what is a TFN?
Tribe Flood Network. A botnet that has been created several years ago that was doing DoS attacks
- Do you think that AI will allow for attacks that are unstoppable?
We need to improve adaptation. AI response to AI attacks.

3. Another attacks

- Reflections attacks
  - Uses different protocols, e.g. UDP or TCP/SYN
  - Future variation creates a loop between intermediary and the target
  - Quite easy to filter and block

- Amplification Attacks
DNS Amplification is a variant of reflection attack

- The attacker sends DNS query with a spoofed IP address of the target machine, the intermediates respond with a DNS responses to the target machine
- Using a DDoS to send intermediate requests to many mediums and having those intermediates send responses to the target machine cause the system to fail.

4. How DNS works

- From symbolic to IP Address, e.g. www.colostate.edu to XXX.XXX.XXX
- Distributed system, has mail servers, domain servers, etc.
- Every network will have information about DNS servers
  - Some called caching server
  - Other - ReServers
- If it doesn’t have info locally - it check if it can call Root DNS servers, in a hierarchical fashion
  - Root DNS - I don’t know what www.colostate.edu, but I know IP for domain .edu
  - .edu DNS server might have information for that
- and so on
- Response to the query can be as small as 512-byte request, or it can be as large as 4000 bytes
  - Object for DoS attack, spoofing for a lot of responses, large responses against victim machines

Socrative:

- How practical is it to contact everyone known to be in a botnet to clean their computers?
  We don’t know layers of zombies. Not easy to identify everyone who is suspect to botnetting
- Are there any other equal or more affective defenses against a SYN flood attack other than the SYN cookie approach
  Problem with SYN cookie approach - it needs modification to TCP stack. We can not change globally. The can not be completely prevented.
- What are the legal repercussions for naively compromising another machine?
  Varies from countries to countries. F.e. if you’re compromising a CSU machine, you’re out of CSU, violation of the academic code. Requirements for sysadmins: report to agencies about the attack. CERT. They globally cooperate

5. Defending from DoS attacks

- May not be a DoS attack
- High traffic volumes may be legitimate
  - Result of high publicity, e.g. “slash-dotted”
  - Or to a very popular site, e.g. Olympics etc
- Or legitimate traffic created by an attacker
- Three lines of defense against DDoS:
- Attack prevention and preemption
- Attack detection and filtering
- Captcha a good example of identifying a human
- Attack source traceback and identification

### Responding to attack
- Contact internet authorities ISP
- Need traffic filter upstream
- Use blacklist/whitelist
- Identify type of attack
  - Prevents future attacks

**Socrative:**
- can dummy systems be used to redirect a flooding attack and thus defend against the attack?

Yes, this is a strategy. In fact. Honeyports/honecomb systems can be used and installed. But there is a cost